Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1346 11/18/11

~ Health Care Data Danger ~ People Are Talking! ~ Zynga Makes Demand!
~ Net Tax A States Right? ~ Norway Sees Data Breach ~ UK To Test Its Banks!
~ Feds Gunning for Google ~ Mortgage Scams Stopped! ~ GameStop Is Upbeat!

~ Facebook Flood of Spam! ~ Kindle Fire Is $ Loss! ~ Intel 4004 Turns 40!

-* SOPA Is Form of Censorship? *-
-* Hearing on Facebook Tracking Wanted *-
-* PC With 4 Million Patients' Data Is Stolen *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Well, it's just me and the three dogs for the weekend. It's not as thrilling as it might sound; two of our "kids" have terminal illnesses, so they require various kinds of care which will keep me busy all weekend. But, these things one has to do for family members of all kinds.

It seems our Indian Summer has taken a short dip lately, and it's been bone-chilling cold the past couple of days. Not to fear, they've been predicting a bounce-back for temperatures starting this weekend, so I'm looking forward to that. Sure, I'll be cleaning leaves for a bit, but it's that time of the year!

Before I forget, all of us here at A-ONE wish you all a terrific Thanksgiving holiday next week! I know I speak for Joe in telling you this is one of our most favorite holidays - plenty of turkey and all the fixings that go along with it! We'll be spending a quiet day ourselves this year, and hoping to be able to relax and enjoy the day.

Until next time...

=~=~=~=

->In This Week's Gaming Section - Zynga: Return Stock or Be Fired!
""""""""""""""""""""""""""""""""" GameStop Upbeat on Holiday Sales!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

GameStop Upbeat on Holiday Sales

GameStop Corp said holiday sales were off to a strong start, easing concerns that recent data showing a slowdown in the industry would hurt the video game retailer.

Sales of traditional video game products such as consoles have been struggling globally as gamers turn to lower-priced online games and spend more time gaming on tablets and phones. GameStop has weathered the trend by focusing on selling used games to console owners.

The company on Thursday said it expects fourth-quarter earnings of $1.66 to $1.76 per share, compared with an average Wall Street estimate of $1.74, according to Thomson Reuters I/B/E/S.

It issued the forecast after reporting third-quarter earnings that met expectations. Its shares were slightly lower, stabilizing after a major sell-off earlier in the week.

Chief Executive Paul Raines told Reuters in an interview that while its customers appeared to be under pressure in the third quarter, the fourth quarter "is off to a great start."

"Consumers and gamers have met our expectations. We were pretty bullish. The holiday titles are off to great start," Raines said.

He added that GameStop’s "buy, sell, trade" model of selling new games and offering to buy back used games has benefited the company even as consumers cut back on spending.

Shares of GameStop were down 1 percent in morning trading. The shares fell 10 percent in the first three trading days this week as Wall Street braced for poor third-quarter results.

The shares dropped after the NPD research firm released data last Friday showing that sales of new video games were not as strong in October as Wall Street had expected.

"There was a lot of concern GameStop would have a huge miss ... but what they reported on Thursday wasn’t as bad as feared," said Sterne Agee analyst Arvind Bhatia.

GameStop said sales of Electronic Arts Inc’s "Battlefield 3" and Microsoft Corp’s "Gears of War 3" helped its results.

Sales rose 2.5 percent to $1.95 billion, just shy of the average Wall Street forecast of $1.96 billion.

Net income slipped 1 percent, to $53.7 million from $54.3 million a year earlier.

Earnings per share were boosted by the company’s repurchase of 1.92 million shares in the quarter. Earnings per share rose to 39 cents from 36 cents a year earlier, matching analysts’ average forecast, according to Thomson Reuters I/B/E/S.

On Thursday, Activision Blizzard, the largest U.S. video game publisher, said its hit game "Call of Duty: Modern Warfare 3" set a new industry record by generating $775 million in sales in its first five days in stores in November.

Zynga to Employees: Give Back Our Stock Or You'll Be Fired

Attracting top employees can be difficult for cash-strapped startups. So, in many cases, they give out company stock to supplement salaries that employees might feel is below-market.

Zynga followed that strategy. But now the CityVille and FarmVille maker apparently wishes it hadn't, according to a new report.

Citing industry sources, The Wall Street Journal reported today that Zynga CEO Mark Pincus, along with his top executives, decided last year as they were preparing for an initial public offering (IPO) that they had given out too much stock to employees. But rather than accept that reality, the executives reportedly tried a different tactic: demand employees give back not-yet-vested stock or face termination.

In order to determine which employees would be asked to give stock back, Pincus and his executives tried to pinpoint workers whose contributions to Zynga - in the execs' eyes - didn't necessarily justify the potential cash windfall they could receive when the company went public, the Journal claims. One Journal source said that Zynga executives were especially concerned with not creating a "Google chef" scenario.

That reference relates to Google's 2004 IPO when one of the company's chefs, who was hired in the firm's early days, walked away with $20 million worth of stock after the shares went public.

After finding people to target, the Journal's sources say, Pincus offered his ultimatum. However, as one might expect, he faced some anger from employees who didn't believe they should be required to give back the stock. The Journal cited two employees - one who has left Zynga and another who still works with the company - who hired attorneys to reach a settlement that saw them give up some, but not all, of the unvested shares.

Although Zynga's decision might be met with some criticism, the firm's executives reportedly justified their strategy by saying it was best for the company. With the unvested shares, the executives believed they could attract more top talent with the promise of stock.

Speaking of stock, the public might soon have a chance to own part of the social-gaming company. Earlier this month, Bloomberg reported that Zynga was planning to go public after Thanksgiving. The company is expected to raise up to $1 billion in an IPO.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Tumblr, Firefox and Reddit Censor Websites to Protest SOPA

Tumblr, Firefox and Reddit drew broad black lines on their websites Wednesday to protest a proposed U.S. law that Internet companies have dubbed "censorship" and entertainment companies "piracy protection."

Their symbolic design tweaks coincide with what several open Internet advocacy organizations have declared American Censorship Day - a day some of the Internet's biggest web companies have dedicated to encouraging users to speak out against the Stop Online Piracy Act (called the Protect IP Act in the Senate). The bill strengthens the U.S. Justice Department's power to go after websites that host disputed copyright material and makes sites such as YouTube and Tumblr that host such user-generated content liable for copyright violations.

Tumblr has blacked out all user-generated content you see when you first log in. When you click on the gray lines to investigate, you're told: "Congress is holding hearings today and will soon pass a bill empowering corporations to censor the Internet unless you tell them no," and then have an option to leave a phone number to be connected to your elected representative.

If you do so, you'll receive a phone call from Tumblr CEO David Karp (or at least a recording of his voice) in which he suggests talking points before saying "thank you for doing your part to protect the Internet" and dialing the appropriate phone number.

Mozilla and Reddit are also participating in the so-called American Censorship Day, by censoring their logos, which click through to instructions for contacting representatives.

Other Internet companies that oppose the legislation protested in more traditional ways. Kickstarter published a blog post that explains why it opposes the bill.

"If, say, someone found a single instance of copyright infringement on Kickstarter, all of Kickstarter - every project - could be taken down until it's removed," the post says, "As you can imagine, this would be disastrous for everyone involved, and it would punish an entire community for the bad behavior (or honest mistake) of one person."

AOL, eBay, Facebook, Google, LinkedIn, Mozilla, Twitter, Yahoo and Zynga delivered a letter to members of the U.S. Senate and House of Representatives that argues SOPA "pose[s] a serious risk to our industry's continued track record of innovation and job creation, as well as to our nation's cybersecurity." On Wednesday, they ran the letter as a full-page ad in the New York Times.

"The solutions are draconian,'' Google Chairman Eric Schmidt said during an appearance at the MIT Sloan School of Management, according to The Christian Science Monitor. "There's a bill that would require (Internet service providers) to remove URLs from the Web, which is also known as censorship last time I checked.''

Have the various protests around the web caused you to get involved in supporting or opposing SOPA? What do you think of proposed legislation?

At Web Censorship Hearing, Congress Guns for "Pro-Pirate" Google

The House Judiciary Committee held an important hearing on the Stop Online Piracy Act with a hugely stacked deck of witnesses; Google's lawyer was the only one of the six to object to the bill in a meaningful way. And it wasn't hard to see why. This wasn't a hearing designed to elicit complex thoughts about complex issues of free speech, censorship, and online piracy; despite the objections of the ACLU, dozens of foreign civil rights groups, tech giants like Google and eBay, the Consumer Electronics Association, China scholar Rebecca MacKinnon, hundreds of law professors and lawyers, the hearing was designed to shove the legislation forward and to brand companies who object as siding with "the pirates."

How low was the level of debate? The hearing actually descended to statements like "the First Amendment does not protect stealing goods off trucks" (courtesy of the AFL-CIO's Paul Almeida).

Right from the start, the knives were out for Google. Committee Chairman Lamar Smith (R-TX) made it only halfway through his opening statement before asserting that "one of the companies represented here today has sought to obstruct the Committee s consideration of bipartisan legislation. Perhaps this should come as no surprise given that Google just settled a federal criminal investigation into the company s active promotion of rogue websites that pushed illegal prescription and counterfeit drugs on American consumers."

SOPA would require search engines, payment processors, ISPs, and ad networks to block access to "rogue websites" on a judge's order. While critics have raised serious concerns about how this could affect the Internet's domain name system, affect free speech, and sweep in a host of legal sites, the bill's backers suggested that it was really just about money. Google didn't want to stop piracy because it made so much money from it.

"Given Google s record, their objection to authorizing a court to order a search engine to not steer consumers to foreign rogue sites is more easily understood," Smith said. (Much later in the hearing, a fired-up Zoe Lofgren [D-CA] said that "impugning the motives of the critics rather than engaging in the substance is a mistake" and that she was troubled by the panel's makeup.)

As for the panelists, most portrayed SOPA as eminently reasonable. And hey, if SOPA breaks something as important as the move to the more secure DNSSEC protocol, no problem - we can just rewrite the protocol.

"This argument [that SOPA will harm DNSSEC deployment] conveniently ignores not only the history of the creation of DNSSEC but also the very nature of Internet protocols, which is simply this: when new developments or circumstances require changes to these codes, the codes change," said MPAA's Michael O'Leary. Putting Hollywood in charge of setting Internet protocol standards: what could possibly go wrong?

It was up to Google alone to make the argument that SOPA's definition of "rogue sites" is poor, that its remedies are extreme, and that plenty of legitimate sites could be targeted. One has only to think of YouTube, which even without SOPA is being sued by Viacom for $1 billion and would certainly have been hammered years ago under SOPA's crazy language (sites

can be dismantled under SOPA if they take "deliberate actions to avoid confirming a high probability of the use of the US-directed site to carry out acts" of infringement. What does that even mean? And how does it fit with existing robust safe harbors for user-uploaded content sites?)

O'Leary of the MPAA smirkingly took on his (largely absent) opponents by saying that SOPA critics were engaged in hypocritical hyperbole and were pro-piracy - as though the long history of the US content industries had just disappeared down the memory hole (Jack Valenti, anyone? The VCR as Boston Strangler? The reason "Hollywood" is in California at all? Rampant 18th and 19th century book piracy? Attacks on HDTV? Attacks on the DVR? Attacks on MP3 players?)

Groups that weren't invited to speak at the hearing vented afterwards. "This lack of speaking and listening has been a continued frustration and led to such a flawed bill," said CCIA chairman Ed Black. "I d liken it to killing mosquitoes with an uzi, but at least the uzi hits its target. This bill will fail to actually stop traffic to infringing sites and will Balkanize Internet traffic, sending the real pirates to foreign DNS servers that can t easily be monitored."

The Consumer Electronics Association, which was apparently denied a chance to participate in the hearing, also pulled no punches. "The bill attempts a radical restructuring of the laws governing the Internet," said CEO Gary Shapiro. "It would undo the legal safe harbors that have allowed a world-leading Internet industry to flourish over the last decade. It would expose legitimate American businesses and innovators to broad and open-ended liability. The result will be more lawsuits, decreased venture capital investment, and fewer new jobs. The significant potential harms of this bill are reflected by the extraordinary coalition arrayed against it. Concerns about SOPA have been raised by Tea Partiers, progressives, computer scientists, human rights advocates, venture capitalists, law professors, independent musicians, and many more. Unfortunately, these voices were not heard at today's hearing."

Over in the Senate, people like Ron Wyden (D-OR) watched the "not entirely fair and balanced" hearing with horror. Wyden, who helped author the key Internet safe harbors that have keep sites like Google, Yahoo, and eBay from being sued into oblivion for the actions of others, submitted a statement of his own. "We took the opportunity to pass a law that said that neutral parties on the net are not liable for the actions of bad actors," he wrote. "So now, as we again debate Web censorship, let's ask ourselves: what next generation of innovations won't be realized if we backtrack on that principal now? Yes, the Internet needs reasonable laws and bad actors need to be pursued, but the freedoms of billions of individual Internet users should not be sacrificed in the interest of easing that pursuit."

Perhaps the irony in all this is that Hollywood itself emerged from a world of piratical behavior to become a dominant American industry - but draconian IP enforcement could have stagnated the industry for decades. In the same way, today's piracy problems can certainly be dealt with in a much more measured fashion; protecting Hollywood now simply can't be worth killing off the next YouTube. As for the truly bad actors, even Google supports measures to go after their sources of revenue with a court order.

Lawmaker Wants Hearing on Facebook Tracking

Sen. Jay Rockefeller (D-W.Va.), chairman of the Commerce, Science and Transportation Committee, said Wednesday he would hold a hearing to look into reports that Facebook tracks its users on the Web after they log out.

"No company should track customers without their knowledge or consent, especially a company with 800 million users and a trove of unique personal data on its users," Rockefeller said in a statement. "If Facebook or any other company is falsely leading people to believe that they can log out of the site and not be tracked, that is alarming."

Facebook spokesman Andrew Noyes said the company uses cookies to personalize content and keep accounts secure.

"When someone logs off of Facebook, we delete certain cookies and reduce the amount of information we receive when the person visits websites that contain social plug-ins such as the Like button," he said in an emailed statement. "We have made these practices clear in our Privacy Policy and Help Center since the launch of social plug-ins. We appreciate Sen. Rockefeller’s interest in protecting consumer privacy and look forward to discussing this with him."

He also said that Facebook does not sell users’ information to third parties and deletes or anonymizes data within 90 days.

In September, the Electronic Privacy Information Center and other privacy watchdogs asked the Federal Trade Commission to investigate Facebook’s tracking of users after they log off the service to see if it harms consumers and invades their privacy.

At the time two other lawmakers, Reps. Edward Markey (D-Mass.) and Joe Barton (R-Texas) raised concerns in a letter to FTC Chairman Jon Leibowitz. The two lawmakers, who have aggressively pursued Facebook on privacy issues, said at the time they were concerned that Facebook is tracking users without their permission.

The issue surfaced again Wednesday in USA Today.

Computer With Info on 4 Million Patients Stolen in California

A Northern California physicians network says a computer stolen last month contains personal information on more than 4 million patients dating back to 1995.

The Sacramento Bee reports the database includes the names, addresses, email addresses, birthdates, telephone numbers and insurance information of 3.3 million Sutter Medical Foundation patients.

Information on another 943,000 patients also includes medical record numbers, dates of services and a description of medical diagnoses and procedures.

Officials at the Sacramento-based not-for-profit network say the data did not include patient financial records, Social Security numbers, health plan identification numbers or medical records.

Affected patients are being notified by mail if their information was compromised.

Sutter says it’s speeding up efforts to encrypt all its computers, but the stolen desktop computer’s data was not encrypted.

Theft of Data on 4 Million Patients Part of Wider Problem

The theft of a computer containing information on more than 4 million patients of a major Northern California health care provider may be among the largest breaches of health care data in recent years, but it’s far from the only incident of its kind.

Over the last two years, health care organizations have reported 364 incidents involving the loss or theft of information ranging from names and addresses to Social Security numbers and medical diagnoses on nearly 18 million patients - equivalent to the population of Florida.

A thief stole medical information on more than 4 million patients of Sacramento-based Sutter Health last month by the simple act of breaking a window with a rock at the affiliated Sutter Medical Foundation. Stolen over the weekend of Oct. 15 were monitors, keyboards and a desktop computer containing patient information dating to 1995.

Employees reported the theft to Sacramento police when they returned to work that Monday, Oct. 17, said Sgt. Andrew Pettit, but they didn’t notify the public until Wednesday, a month later. The company said in announcing the theft Wednesday that some patients might not receive mailed notices until early next month.

"If that machine is that valuable, then there should be more security measures where that is protected. There’s got to be something in place to make sure that that doesn’t happen," Pettit said.

Police were investigating the burglary as a routine smash-and-grab property theft, he said, and so far there is no indication that the information in the computer has been used.

Since federal health care data breach notification rules took effect in 2009, Health and Human Services records show that the Sutter theft was exceeded only when the U.S. military’s health insurance program lost backup tapes in September containing information on more than 4.9 million patients.

While Sutter said the computer was password-protected, the data on patients was not encrypted, drawing criticism from privacy and computer security experts.

"Had this data been encrypted, you and I wouldn’t be having this discussion. It would be a nonissue," said Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit consumer education and advocacy organization based in Sacramento.

On a computer in which data is encrypted, a user would typically have to enter another password in addition to the computer’s general password to access that specific data.

Information on about 3.3 million patients included name, address, date of birth, phone number, email address, medical record numbers and the name of the patient’s health insurance plan. Information on another 943,000 patients also included dates of services and descriptions of medical diagnoses and procedures.

Sutter spokesman Bill Gleeson said the company waited a month because it took that long to determine which patients’ information was contained in the computer. The company properly notified the federal government as well as others beyond what was required, he said, and hired a private investigator who so far has turned up no leads on the stolen computer.

The stolen computer was scheduled to be encrypted "very soon," he said. Sutter initially concentrated on encrypting hand-held and laptop computers because those were deemed more likely to be lost or stolen.

"We deeply regret that that computer was stolen and that information about our patients was included. We have no reason to believe that computer was taken for that information," he said. He added that Sutter has heightened security for the building and was working on encrypting all of its computers.

The stolen computer did not contain patient financial records, Social Security numbers, health plan identification numbers or actual medical records, Sutter said.

Though encrypting patient information is "highly recommended" by the federal government, Verizon health care and data security expert Dr. Peter Tippett said the health care industry lags behind the financial and high-tech industries by 10 to 15 years when it comes to protecting personal data.

"Overall, the health care system needs a lot of work at being more secure," Tippett said.

In most cases, Tippett said, computer thieves are simply looking to make a little cash reselling the stolen computer itself. Sometimes they may try to ransom the computer back to its original owner. If the data itself is accessed, usually by organized crime operations, he said criminals would generally try to use it to blackmail prominent people with potentially embarrassing diagnoses or steal patients’ identities to fraudulently bill health insurers for medical procedures that weren’t really performed.

The worst consequence an average patient could expect would be a bill for a co-pay for a procedure they never received, he said.

Tippett said blaming any incident of identity theft on the stolen Sutter computer would be tough. If exploited, the patient information on the stolen computer would simply be added to the insecure data available on most everyone already floating around on the world’s computer networks.

"It’s real. It will hurt some people. But it won’t hurt the average person in Sacramento," he said.

Sutter appears to have followed state and federal law and faces little investigation at least from California, officials said, particularly if no damage results to individuals.

California Department of Managed Care spokeswoman Denise Schmidt said her

agency is "looking into whether there may be an impact," but she couldn’t say what that might entail.

State Department of Insurance spokesman Dave Althausen said his department would only become involved if there are fraudulent insurance claims as a result.

Sutter notified the state Department of Public Health, but didn’t need to, said department spokesman Ralph Montano. His department would only have jurisdiction if the breach was from a hospital or nursing home, he said, not a medical foundation or physician services group.

Joanne McNabb, chief of the California Office of Privacy Protection, said Sutter was only required to notify the U.S. Department of Health and Human Services, which it did within the required 60 days.

It was also required to notify affected patients in "the most expedient time possible without unreasonable delay," she said, quoting a 2008 state law. A one-month delay might be reasonable because it could have taken that long to determine what information was on the computer, she said.

Consumers should watch out for bogus medical procedures showing up on health care notices, and should be careful not to be caught by crooks using their information to seek Social Security numbers or other information, she said. But she said the data on the computer is relatively limited in the damage that could be done with it directly.

Internet Tax A States’ Rights Issue

Before he became a U.S. senator, Mike Enzi ran a shoe store and was mayor of Gillette, in the heart of Wyoming’s coal country.

Making payroll as a small businessman and sticking to a budget as a local government official drives Enzi now as he leads a bipartisan group of senators pushing legislation to help states recover billions in sales taxes they’re losing to Internet sales.

"We need to fix this so that the loophole doesn’t exist anymore, and that will take care of those local governments without the federal government having to raise more taxes for them," Wyoming’s senior Republican senator told The Associated Press in an interview this week.

Under the Marketplace Fairness Act, the 45 states with state sales taxes could require online retailers that sell more than $500,000 a year to collect sales taxes for them regardless of where those retailers are headquartered. Internet retailers currently must collect sales tax only for those states they have a presence in, such as a store or an office.

In some cases, online consumers are required to pay tax to their home state but don’t always do so.

States striving to make ends meet in tough times will lose more than $23 billion in uncollected sales taxes in 2012, the National Conference of State Legislatures estimates.

"I used to be a retailer, and I find it discouraging when somebody comes in and they pick something up and they say, ’Now if you’ll sell it to me

without the sales tax, I'll buy it,'" Enzi said.

"And you say, 'Well that would be illegal, I can't do that.' And they come up with some alternate plans for how you could ship it out of state for them. But if you're a brick-and-mortar business, if you actually live in the community, then that's not an option. So they go and they buy it online so they don't have to pay sales tax."

Enzi said he commonly hears from Wyoming retailers that addressing the tax issue is essential for main street businesses that provide jobs and help their communities. Under the bill, state governments would share tax revenues with local governments based on address records of people ordering goods online.

Enzi and Sens. Dick Durbin, D-Ill., and Lamar Alexander, R-Tenn., lead the group of 10 U.S. senators behind the bill.

Internet retailer Amazon.com Inc. has said it supports the bill. The company fought taxation efforts in several states but said it would prefer a federal solution.

Online auction company eBay Inc. opposes the legislation, saying it would place an unfair burden on small retailers to collect and remit sales taxes around the country. Enzi said he believes that exempting businesses with less than $500,000 in sales addresses those worries.

Enzi said he doesn't accept the argument from some Internet companies that they shouldn't have to collect taxes for states in which they don't have a physical presence or use state services.

"They have a presence there, otherwise people wouldn't be able to buy from them," he said. "It's not a brick-and-mortar presence in which there's property tax they have to pay as well. They don't have to pay the in-state employee fees. All of those are things that help to keep things going. I also used to be a mayor, so I know that this is a huge infrastructure and jobs bill."

Enzi also doesn't accept the argument that states should simply learn to live with less.

"Live with less, so that out-of-state retailers can live with more?" he asked. "No, I don't think that's a legitimate one to ask your out-of-state businesses to put your in-state businesses out of business."

The senator said he and his colleagues long have wrestled with the tax issue - and there's a good chance this bill can resolve it.

"I'm very optimistic this time," Enzi said. "I've been working on it for a number of years, and a drastic change that we made in the bill was to make it a state's rights issue, and each state will have to pass a law in order to be part of this."

UK To Test Banks with Simulated Cyber Attack

Banks in London, already on high alert for how to deal with a break-up of the euro zone, will on Tuesday be tested to see how they would cope with a cyber attack on their operations.

In one of the largest exercises of its kind in the world, involving thousands of staff and dozens of firms, Britain's financial supervisors will assess how banks will cope with a collapse of telecoms, internet and other systems.

They will be also be tested for a simulated transport disruption during the Olympic Games.

It comes just as banks are ramping up their own disaster scenarios, such as Greece's exit from the euro, bankers said.

Eighty-seven firms will take place in next week's test, which is run by the Financial Services Authority, the UK Treasury and the Bank of England.

The last exercise in November 2009 tested firms' ability to cope with widespread flooding and snow, while one in 2006 simulated a flu pandemic. It can simulate an abrupt collapse of critical infrastructure and staff absence, or test operations over a longer crisis.

The exercises allow banks to see how they might sustain their operations, forcing them to relocate to back-up sites for example, or reboot systems.

Last time firms ranging from HSBC and Goldman Sachs to the London Metals Exchange and Skipton Building Society took part.

There is already rigorous testing of systems going on, including for a possible euro zone breakup, as part of an ongoing risk management process that has stepped up considerably in recent years, bankers said.

One head of Greece at a major bank said that all financial firms in the country had rigorously worked through dozens of scenarios and various degrees of sovereign default.

Banks are constantly testing their capital, liquidity and operations, such as payments systems, for the risk of problems. As the euro zone breakup risk has risen, that feeds into the checks.

"Everyone is aware of the potential issues that could arise at the moment. Some are harder to stress than others, but you can make sure your operations are solid and you've got the liquidity and capital in place," a person at one UK bank said.

Norway Hit by Major Data-Theft Attack

Data from Norway's oil and defense industries may have been stolen in what is feared to be one of the most extensive data espionage cases in the country's history, security officials said Thursday.

Industrial secrets from companies were stolen and "sent out digitally from the country," the Norwegian National Security Authority said, though it did not name any companies or institutions that were targeted.

At least 10 different attacks, mostly aimed at the oil, gas, energy and defense industries, were discovered in the past year, but the agency said it has to assume the number is much higher because many victims have yet to realize that their computers have been hacked.

"This is the first time Norway has unveiled such an extensive and widespread espionage attack," it said.

Spokesman Kjetil Berg Veire added it is likely that more than one person is behind the attacks.

The methods varied, but in some cases individually crafted e-mails that, armed with viruses, would sweep recipients' entire hard-drives for data and steal passwords, documents and confidential documents.

The agency said in a statement that this type of data-theft was "cost-efficient" for foreign intelligence services and that "espionage over the Internet is cheap, provides good results and is low-risk." Veire would not elaborate, but said it was not clear who was behind the attacks.

The attacks often occurred when companies were negotiating large contracts, the agency said.

Important Norwegian institutions have been targeted by hackers before.

In 2010, some two weeks after Chinese dissident and democracy activist Liu Xiaobo was named that year's Nobel Peace Prize winner, Norway's Nobel Institute website came under attack, with a Trojan Horse, a particularly potent computer virus, being installed on it.

Other attacks on the institute in that same period came via email, containing virus-infected attachments.

Facebook Warns of Recent Wave of Spam

Facebook said Wednesday that it has stopped most of the spam that has flooded many users' pages with pictures showing graphic sex and violence.

The social-networking company urged its 800 million-plus users to remain vigilant to keep their accounts from being hijacked.

That includes reporting suspicious links on friends' pages and not clicking on links that offer deals that are too good to be true.

Social-networking sites are popular targets for spammers because people are more likely to trust and share content that comes from people they know. This makes spam, scams and viruses easy to spread.

Still, Facebook says less than 4 percent of content shared on the site is spam. By comparison, about 74 percent of email is spam, according to security firm Symantec, though the bulk gets filtered out before reaching the inbox.

Over the past couple of days, many users have complained about finding links on their Facebook pages taking them to images depicting jarring violence and graphic pornography. Although the way the latest spam messages spread isn't new, their content is more shocking than the typical scam enticing a free iPod shuffle.

The latest attack tricked users into clicking on links by offering some sort of promise - free plane tickets, a fun new video or answers to a

quiz, for example, said Vikram Thakur, principal security response manager at Symantec.

Clicking on the link took users to a page that asked them to copy and paste a line of malicious JavaScript programming code into the address bar of their Web browser.

"Pasting that little message will pick up a message or picture from whatever website the JavaScript is posting to," Thakur said, adding that it doesn't matter what type of browser people use.

The content is then posted on the users' Facebook page, usually without their knowledge. It spreads further when their friends then click on those links, thinking that it was posted by the user on purpose.

Facebook said no user data or accounts were compromised during the attack.

It urged users not to cut and paste unknown code into a browser's address bar. They should always use an up-to-date browser and report any suspicious content on the site.

While the site scans malicious links against security databases and blocks those known to lead to spam, it can't stop people from copying and pasting text manually into their Web browser.

That's where user vigilance comes in.

Thakur said users should be suspicious by the mere fact that someone is asking them to copy and paste something that Facebook is not permitting to be clickable directly.

Facebook said it built enforcement mechanisms to quickly shut down the malicious pages and accounts that attempt to exploit the vulnerability.

"Our team responded quickly and we have eliminated most of the spam caused by this attack," Facebook said in a statement. "We are now working to improve our systems to better defend against similar attacks in the future."

Government Closes Mortgage Scams Tied to Google

The federal government has shut down dozens of Internet scam artists who had been paying Google to run ads making bogus promises to help desperate homeowners scrambling to avoid foreclosures.

The crackdown announced Wednesday renews questions about the role that Google's massive advertising network plays in enabling online misconduct. It may also increase the pressure on the company to be more vigilant about screening the marketing pitches that appear alongside its Internet search results and other Web content.

The criminal investigation into alleged mortgage swindlers comes three months after Google agreed to pay $500 million to avoid prosecution in Rhode Island for profiting from online ads from Canadian pharmacies that illegally sold drugs in the U.S.

A spokesman for the U.S. Treasury Department division overseeing the

probe into online mortgage scams declined to comment on its scope other to say it’s still ongoing.

Google Inc. also declined to comment Wednesday.

No company wants to be tainted by a criminal investigation, but the prospect is even more nettlesome for Google because it has embraced "don’t be evil" as its corporate motto.

That commitment may make it difficult for Google to fend off a call by Consumer Watchdog to donate the revenue from fraudulent mortgage ads to legitimate organizations that help people ease their credit problems. Consumer Watchdog is an activist group that released a report in February asserting that Google was profiting from ads bought by mortgage swindlers.

"Google should never have published these ads, but its executives turned a blind eye to these fraudsters for far too long because of the substantial revenue such advertising generates," said Consumer Watchdog’s John M. Simpson, a frequent critic of the company.

To fight future abuse, Google has suspended its business ties with more than 500 advertiser and agencies connected to the alleged scams, according to the U.S. Treasury Department’s Office of the Special Inspector General for the Troubled Asset Relief Program.

The evidence collected in the current investigation led to the government’s closure of 85 alleged mortgage scams. The identities of the businesses and people involved in the scams weren’t disclosed Wednesday.

The con artists are accused of duping people into believing they could help lower their home loan payments under a government-backed mortgage modification program created to reduce the foreclosures that have made it more difficult for the slumping real estate market to recover. The alleged rip-offs typically relied on collecting upfront fees or getting victims to transfer their monthly mortgage payments to the scam artists, according to the Office of the Special Inspector General for the Troubled Asset Relief Program.

In some cases, the swindlers passed themselves off as being affiliated with the government.

Google’s name popped up because the scam artists relied on the company’s vast advertising network to bait their victims. About two out of every three Internet search requests are made through Google, making its ad network a prime outlet for finding people hoping to save their homes, according to Christy Romero, deputy special Inspector General for the Troubled Asset Relief Program.

"The first place many homeowners turn for help in lowering their mortgage is the Internet through online search engines, and that’s precisely where they are being taken advantage of and targeted," she said.

In its February report on the problem, Consumer Watchdog found that Google processed more than 74,000 monthly searches using the term, "stop foreclosure." An ad running alongside the results for that query cost an average of $8.29 per click at the time of the Consumer Watchdog study. The report couldn’t determine how much money Google was making from the ads offering bogus mortgage modifications.

Even after surrendering $500 million to settle the investigation into ads for illegal online pharmacies, Google is still expected to sell more than $35 billion in advertising this year.

Amazon Pays $201.70 To Build $199 Kindle Fire

A teardown of the new Kindle Fire tablet performed by IHS iSuppli researchers found that it costs Amazon $201.70 to make a device that began retailing this week for $199. "Amazon makes its money not on Kindle hardware, but on the paid content and other products it plans to sell the consumer through the Kindle," said Andrew Rassweiler, senior director of teardown services for IHS.

However, the Kindle Fire hardware cost breakdown released by the analyst firm Friday only tells part of the story. Amazon had not disclosed what it is costing the online retail giant to roll out the tablet from a software perspective - including software design, development and testing.

"We can safely assume that launching such devices from a software perspective requires a serious long-term commitment to morphing Android into what Amazon is looking for," said Al Hilwa, director of applications software development at IDC.

According to Hilwa, a development team of a few hundred people would ultimately be needed to support an ongoing product such as the Kindle Fire, including the requisite maintenance as well as product evolution.

"I have no specific information on this, but I have always imagined that the team working on iOS at Apple, end-to-end, well exceeds a thousand people," Hilwa said. "Doing the estimates for things like that is complex because of shared resources in an organization."

IHS iSuppli noted that its preliminary cost calculations for the Kindle Fire only account for hardware and do not include additional expenses such as software, licensing, royalties, marketing or other expenditures. However, Rassweiler compared Amazon’s strategy of selling its new tablet at a loss to the business models followed by wireless carriers such as AT&T or Verizon.

"They sell you a phone that costs them $400 to $600 or more to make for a price of only $200," Rassweiler said. "However, they expect to more than make up for that loss with a two-year service contract."

According to IHS, the new Kindle Fire’s single most-expensive subsystem is its display and touch screen, which has a combined cost of $87 and accounts for 46.9 percent of the device’s total bill of materials. Featuring E Ink’s FFS technology, the displays are being manufactured by LG Display as well as E Ink Holdings.

The dominant semiconductor supplier behind Amazon’s Kindle Fire is Texas Instruments (TI), which supplies the OMAP4430 processor responsible for delivering the new tablet’s core multimedia functionality as well as other parts. TI reaps $24 for every Kindle Fire sold, which is equivalent to 12.9 percent of the device’s total.

TI’s OMAP4430 is also found in a number of other electronic gadgets, including Research In Motion’s PlayBook tablet as well as in smartphones

such as the Motorola Droid Bionic XT875 and LG Optimus 3D P920. The 1-gigahertz dual-core chip features an IVA 3 hardware accelerator as well as an SGX540 3D graphics core, IHS researchers said.

The Kindle Fire’s memory subsystem - which consists of 8GB of eMMC NAND flash memory as well as 4 gigabits of low-power DDR2 DRAM memory - costs Amazon $22.10, or 11.9 percent of the total. According to IHS researchers, Samsung is supplying the NAND flash chips while Japan-based Elpida makes the new Kindle Fire’s DRAM memory components.

Intel 4004, The First CPU, Is 40 Years Old

Four decades ago - November 15, 1971 - Intel placed an advertisement for the first single-chip CPU, the Intel 4004, in Electronic News. Designed by the fantastically-forenamed Federico Faggin, Ted Hoff, and Stanley Mazor, the 4004 was a 4-bit, 16-pin microprocessor that operated at a mighty 740KHz - and at roughly eight clock cycles per instruction cycle (fetch, decode, execute), that means the chip was capable of executing up to 92,600 instructions per second. We can t find the original list price, but one source indicates that it cost around $5 to manufacture, or $26 in today s money.

The 4004 used state-of-the-art Silicon Gate Technology (SGT) PMOS logic - a technique that Faggin perfected at Fairchild Semiconductor in 1968 - the world s first metal-oxide-silicon (MOS) process. This breakthrough allowed the 4004 to have no less than 2,300 transistors and a feature size of 10 micron. By comparison, there are half a billion transistors in a Sandy Bridge chip, and each one is just 0.032 micron. Considering a human hair is around 100 micron, the 4004 was still rather impressive - but irrespective of feature size or transistor count, the fact that it was carved from a single piece of silicon is what made the 4004 truly spectacular. Faggin was so proud of his creation that he even signed the chip ’FF’, which you can see in the top right of the image below.

In real-world use, the 4004’s 92,600 instructions per second equated to the addition of two eight-digit numbers in 850 microseconds, or around 1,200 calculations per second. It s perhaps not surprising that the first use of the 4004 was in the Japanese Busicom 141-PF calculator - and in fact, it was Busicom who originally asked Intel to create the 4004, as its in-house engineers needed 12 integrated circuits to make the 141 calculator work. Busicom actually owned the design of the 4004 and had exclusive rights to its use, but eventually agreed to let Intel sell the chip commercially - and thus the fateful appearance of that 1971 Electronic News ad.

Despite the 4004’s success - and the popularity of its 8-bit successors, 8008 and 8080 - Intel was still very much a DRAM and SRAM company at the time. It wasn t until the late 70s with the 8088, which powered the IBM PC and its clones, that Intel decided to make the shift towards microprocessors, and as we now know, the rest is history.

Florida Craigslist Jobseeker Found Dead in Ohio Grave

A jobseeker from Florida who responded to a bogus Craigslist ad for a job

on a southeast Ohio cattle farm was found dead, buried in a shallow grave, and another from South Carolina was shot but escaped by running away through the woods, a sheriff said Thursday.

Noble County Sheriff Stephen Hannum said two men were taken into custody after cadaver dogs found the body of the Florida man this week in a grave in a remote area outside Caldwell, a small village about 80 miles east of Columbus.

The Akron Beacon Journal identified the two as a 16-year-old student from Stow-Munroe Falls High School and a 52-year-old Akron man.

The adult is being held in the Summit County Jail on $1 million bond, the newspaper said. His attorney could not be reached for comment. No further information was available about the juvenile.

Hannum said the search was undertaken after the South Carolina man escaped from the area on Nov. 6 and notified police, who later found a hand-dug grave authorities believe had been meant for him.

An autopsy on the Florida man was being performed Thursday in Licking County, outside Columbus, and Hannum said names of the suspects and victims were being withheld until at least Friday.

Authorities received a call five days after the South Carolina man was shot from the Florida man’s twin sister, concerned that her brother had not been heard from since Oct. 22 in Parkersburg, W.Va., the sheriff said. The twin, in Boston, said her brother had responded to what she believed was the same Craigslist ad, which sought a caretaker for cattle on a 688-acre farm.

The sheriff said the South Carolina man had been told to carry his belongings to Ohio because he’d be living at the farm, and robbery was believed to be the motive.

"It seems that this was just a ruse to lure victims into the trap, most likely to commit a murder and relieve the deceased of their personal property," Hannum said.

He said it was unknown how long the ad had been online or how many people may have responded.

The sheriff said the call prompted officers to return to the remote area, where they found the grave believed to have been intended for the South Carolina man.

"A grave obviously had been dug that we assume had been dug for him, but he was shot and wounded and he got away," Hannum said. "We brought in cadaver dogs thinking that a possibility that the person that was advertising on Craigslist and lured this guy down here may very well have lured someone else to the same area. Our hunch was correct."

The cadaver search began Monday, and officers found the body the following day. The suspects were arrested Wednesday in Summit County, in northeast Ohio, about 90 miles away.

Hannum said the South Carolina man had hidden in the woods for about seven hours with a gunshot wound to his arm.

The man eventually made his way to a house about 2 miles away. He told

police he had been walking in a wooded area with one of the men when he heard a gun cock and turned to see a firearm pointed at his head. He pushed it away and ran. He said multiple shots were fired and he was hit once.

The man said he had met the others for breakfast and later rode with them in a vehicle, believing he was headed to the farm, until he was told a landslide had closed the road and entered the woods on foot.

The Craigslist website, which features free classified ads for housing, jobs, personal announcements, items for sale and services, among other things, has been blamed for a number of deaths, including that of a New York City masseuse who authorities say was killed in 2009 by a Boston medical student she met through the site.

More recently, in September, the last of four defendants was sentenced in the 2010 killing of a Tacoma, Wash.-area man in a home robbery during which the group pretended to be interested in a diamond ring advertised on Craigslist.

Craigslist founder Craig Newmark has urged people to take precautions when using the site.

"It’s been devastating to see that it can also be used by bad people to take cruel advantage of others," he said in 2009 at a ceremony honoring a Minnesota woman who died after responding to a phony ad for a baby sitter.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.